

REMARKS

The Office Action dated May 10, 2007 regarding the above-identified application has been carefully considered; and the claim amendments above together with the remarks that follow are presented in a bona fide effort to respond thereto and address all issues raised in that Action.

Care has been taken to avoid entry of new matter. Although broadened somewhat, for example, to recite "creating" instead of "dividing" a document, the independent claims have been amended to positively recite verification of the partial documents in a manner crafted to more clearly distinguish over the applied art. Claims 2 and 9, which previously recited examining validity of partial documents, have been cancelled. A number of additional amendments have been made to clarify the independent claims, and several dependent claims have been amended as appropriate to conform the language thereof to the new versions of the respective independent claims. Unless specifically referenced as a distinguishing limitation in a traversal of an art rejection below, it is believed that revised claim language only provides improved grammar or clarity and as such does not narrow the scope of any amended claim.

For reasons discussed below, it is believed that this case is in condition for allowance. Prompt favorable reconsideration of this amended application is requested.

The Office Action included a rejection of previous versions of claims 1, 2, 4-9 and 11-14 under 35 U.S.C. §103 as unpatentable over U.S. Patent No. 6,671,805 to Brown et al. (hereinafter Brown) in view of newly applied U.S. Patent No. 7,174,460 to Horita et al. (hereinafter Horita). Claims 3 and 10 stand rejected under 35 U.S.C. §103 as unpatentable over the combination of Brown and Horita, further in combination with U.S. Application Publication No. 2003/0145197 to Lee et al. (hereinafter Lee). These rejections are traversed on the ground

that the proposed combinations do not satisfy all requirements of either of Applicants independent claims, as presented in the Amendment above.

Independent claim 1 relates to an electronic document management system. The system includes a data creation device for creating an electronic document, including two or more partial documents. A signature device generates items of information, each of which is for verifying validity of a respective one of the partial documents. This device also generates an aggregate of the generated items of information, for use in verifying the validity of the electronic document. Furthermore, the signature device generates a digital signature with respect to the aggregate of the generated items of information. The system of claim 1 also includes a masking device, which masks the electronic document by deleting or modifying one or more partial documents. It should be noted that the masking is done after generation of the items of information and the digital signature. As a result, the items and the signature can be used to verify validity of partial documents excluding any masked partial documents.

The recited system further includes a verification device for verifying the validity of the masked electronic document, that is to say, the document having one or more deleted or modified partial documents. In the system of claim 1, the verification device verifies the digital signature using the aggregate of the generated items of information, and it examines validity of each partial document. The examination of the validity of partial documents includes examining validity of the one or more deleted or modified partial documents. To examine validity of a respective partial document, the verification device verifies the generated item of information for the respective partial document; and it determines whether or not each respective partial document has been deleted or modified, based on the result of the item verification. With such an approach, even when masking (modifying or deleting) one or more partial documents within

an electronic document, the system allows the electronic document to be verified by checking the digital signature and checking the items of information, making it possible to verify the validity of the partial documents and determine whether each respective partial document has been deleted or modified.

Independent method claim 8 recites steps similar to the functions performed by the elements of the system of claim 1, although the wording (and thus claim scope) varies somewhat. In particular, claim 8 requires examining the validity of each of the partial documents of the masked electronic document, including the one or more deleted or modified partial documents. This examining is implemented by verifying the generated item of information for each respective one of the partial documents; and based on a result of the item verifying, determining whether each respective partial document has been deleted or modified.

To appreciate the claim concepts and to confirm support for the amended claim language, it may be helpful to consider Applicants' disclosure by way of an example. As disclosed in the present application, an electronic document is divided into two or more partial documents (e.g. at step 115 in FIG. 4), and items 302 or 304 of information are generated for verifying validity for the respective partial documents. Examples of the items of information include hash functions 302a-302d for the respective partial documents 300a-300d (step 133 in FIG. 6) and signatures 304a-304d for the respective partial documents 300a-300d (step 134 in FIG. 6). The disclosed technique also involves generating an aggregate of the generated items of information for verifying the validity of all the partial documents (step 135 in FIG. 6), and generating a digital signature 303a or 303b to the aggregate of the generated items of information (step 136 in FIG. 6). In the illustrated example of FIG. 2, the unmasked data 2 and signature-related data 4a or the unmasked data 2 and signature-related data 4b are combined and saved as the whole data 3. The

partial documents may be masked, e.g. so that the electronic document is partially rendered private at the time of its disclosure.

Application FIG. 7 shows an example of the verification processing. The validity of the masked electronic document (FIG. 3) can be verified, by verifying the aggregate of the generated items of information using the digital signature (step 141 in FIG. 7). Step 143 is a check the signature-related data 4 to determine the type of signature technique employed in generating the items of information. If hashing was employed, then step 144 is performed to determine the hash values for all the units 300 of the unmasked data 2. Step 145 is performed to verify the units of masking 300 by comparing the hash values certified by aggregate signature verification in step 142 against the hash values determined in step 144. If the two hash values are equal for a respective partial document or ‘unit’ 300, then the validity is certified because the corresponding unit 300 is neither masked nor altered. If, on the other hand, the two hash values are not equal for a respective partial document or ‘unit’ 300, it means that the corresponding unit 300 is masked or altered. By contrast, if the signature technique was used (alternate branch out of step 143), then in step 146, the signature value certified by signature verification in step 142 is used to perform signature verification for each corresponding hash. If signature verification is successful, the validity is certified because each corresponding unit 300 is neither masked nor altered. If, on the other hand, signature verification is unsuccessful, the corresponding unit 300 is masked or altered. The specification discusses these processing steps of Fig. 7, starting on line 11 of page 20 and ending on line 14 of page 22.

Applicants respectfully submit that neither the combination of Brown and Horita nor the combination of Brown, Horita and Lee satisfies all of the recitations of either independent claim 1 or claim 8.

Brown discloses a technique for digitally signing an electronic document by a plurality of signers. Brown's methodology includes identifying a to-be-signed portion of the document corresponding to the signing role of each signer; receiving an indication from each signer to digitally sign the document; and applying the digital signature of each signer to the corresponding to-be-signed portion in response to the indication from each signer. Attention, for example, is directed to the abstract. Brown also teaches masking of portions of the documents. Apparently, the masking is done before signature, as the party that will sign ("the signer") will perceive a "blank" portion of the document 102 when it is displayed unless that party is one authorized to view an access-restricted section. Attention is directed to the discussion of masking and access-restrictions running from line 56 of column 12 to line 12 of column 13. Brown also describes a signature verification service, in the text running from line 9 of column 22 to line 45 of column 23. Apparently, this service can be used to verify the signature associated with each to-be-signed portion of the document. Although Brown might be construed as teaching signatures and masking, as noted the masking apparently is done before signing, not after signature generation as in Applicants' claims.

In Brown, the signing module 108 calculates a message digest, such as a hash value, for a "to-be-signed" portion within the electronic document. A digital signature is applied to the message digest (see e.g. column 9, lines 3-30). A receiver of the document can verify the digital signature for the corresponding "to-be-signed" portion (column 22, lines 9-22). Portions of the document may be encrypted for masking purposes, and it appears that an encrypted portion may be a "to-be-signed" portion, signed by a person authorized to access such a document portion (column 13, lines 8-12). However, it is not seen where Brown, particularly in the text cited in the rejections, would suggest signing or otherwise creating items of information and using the

signatures or other items for verifications of portions of the documents other than those designated as “to-be-signed.” Such a verification of only the to-be-side portions of the electronic document does not involve a determination of whether each respective partial document has been deleted or modified after signature and item generation based on results of the verifying of the generated item of information for each respective one of the partial documents. As a result, Brown does not examine the validity of each of the partial documents of the masked electronic document including the one or more deleted or modified partial documents, in the various ways recited in Applicants’ independent claims.

In addressing former claims 2 and 9, the rejection over Brown in view of Horita points to Brown (citing column 22, line 9 to column 23, line 45) for an alleged disclosure of determining which partial document has been partially deleted or modified by verifying the item of information generated for each respective partial document. However, Brown discloses an electronic document that is composed of one or more to-be-signed portions, access-restricted portions and processing portion (Fig. 1, Fig. 6 and col. 15, lines 17-21). Brown generates a digital signature for the to-be-signed portion to verify the validity of that portion, but Brown generates nothing separately for the access-restricted portion and the processing portion. Although Brown masks the access-restricted portion, Brown does not generate a digital signature specific to that portion, because the portion is already hidden from the signer’s view. It is submitted that Brown cannot verify the validity of each of the partial documents within the electronic document including any masked partial documents, and thus cannot verify the electronic document as a whole where part of the document may be hidden.

In the first art rejection in the latest Action, the Examiner acknowledges that Brown does not disclose a system that generates an aggregate of the items of information, generates a digital

signature to the aggregate and verifies the signature using the aggregate. Instead, the rejection interprets Horita as an alleged disclosure of the aggregate and signature generation and attendant verification. However, Horita discloses a distributed digital signature generation method in which each of the partial digital signature generation parts generates a partial digital signature using a partial signature key different from each other for a hash value of a digital document. Horita mentions nothing of one or more partial documents within the digital document. Hence, Horita would not lead one of skill in the art to generate items of information for partial documents, form an aggregate of such generated items of information and verify the signature using the aggregate. Hence, it is believed that Horita would not lead one of skill in the art to modify Brown as proposed in the rejection. As a result, the combination of Brown and Horita would also fail to meet the claim requirements regarding generating items of information for partial documents, forming an aggregate of the generated items of information and verifying the signature of the aggregate using the aggregate of the items of information.

Further, Horita does not suggest masking one or more partial documents. Even if Horita's digital document was partially masked, that would not be treated as more than just alteration of the document. Hence, Horita would not lead one of skill in the art to modify Brown to perform the masking after signature generation or to examine the validity of each of the partial documents of the masked electronic document including the one or more deleted or modified partial documents, in the ways recited in Applicants' independent claims.

For reasons outlined above, any combination of Brown and Horita would fail to satisfy all of the recitations of either of the pending independent claims. Hence, claims 1 and 8 and the claims that depend therefrom should be patentable over that first combination proposed in the Office Action.

It is respectfully submitted that the addition of Lee to the combination of Brown and Horita, still would not satisfy of the limitations of the independent claims, and as a result that three-reference combination still would not render any pending claim obvious. Lee is cited only for a verification display function. Addition of such a display function to the combination of Brown and Horita still would not overcome the deficiencies of Brown and Horita discussed above relative to claims 1 and 8. Claims 1 and 8 would be patentable over Brown, Horita and Lee, therefore dependent claims 3 and 10 that were rejected over that three-reference combination should also be patentable.

Upon entry of the above claim amendments, claims 1, 3-8 and 10-14 are active in this application, all of which should be patentable over the art applied in the Action. Applicants therefore submit that all of the claims are in condition for allowance. Accordingly, this case should now be ready to pass to issue; and Applicants respectfully request a prompt favorable reconsideration of this matter.

It is believed that this response addresses all issues raised in the May 10, 2007 Office Action. However, if any further issue should arise that may be addressed in an interview or by an Examiner's amendment, it is requested that the Examiner telephone Applicants' representative at the number shown below.

To the extent necessary, if any, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 KEG:apr
Facsimile: 202.756.8087
Date: August 7, 2007

**Please recognize our Customer No. 20277
as our correspondence address.**